UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/890,800	08/03/2001	Noriko Takeda	018773-030	7896

21839 7590 03/14/2005

BURNS DOANE SWECKER & MATHIS L L P
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
WILLIAMS, JEFFERY L	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 03/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/890,800	TAKEDA ET AL.	
	Examiner	Art Unit	
	Williams Jeffery	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-12 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-12 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 03 August 2001 is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 11/29/01, 8/4/03, 11/4/03
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Remarks

Drawings

Figures 13 - 15 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g).

The drawings are objected to under 37 CFR 1.83(a) because they fail to show the proper paths of communication for elements S501, S502, and S503 of Fig. 10 as described in the specification. Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d).

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: reference signs (i.e. A11, A50, B21, B80) are found beginning on page 2, line 25, and are described throughout the entirety of the description.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure

number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

In addition to Replacement Sheets containing the corrected drawing figure(s), applicant is required to submit a marked-up copy of each Replacement Sheet including annotations indicating the changes made to the previous version. The marked-up copy must be clearly labeled as "Annotated Sheets" and must be presented in the amendment or remarks section that explains the change(s) to the drawings. See 37 CFR 1.121(d)(1). Failure to timely submit the proposed drawing and marked-up copy will result in the abandonment of the application.

Specification

The disclosure is objected to because of the following informalities: Specification contains the misspellings of 'security' (page 2, par. 2) and 'invention' (page 8, par. 4). Appropriate correction is required.

35 U.S.C. 112, first paragraph, requires the specification to be written in "full, clear, concise, and exact terms." The specification is replete with terms which are not clear, concise and exact. The specification should be revised carefully in order to comply with 35 U.S.C. 112, first paragraph. Examples of some unclear, inexact or verbose terms used in the specification are: "the number of transferring the communication management table is large", "invention aims to reduce the number of transferring the communication management table" (page. 3), and "a secret key for secret key communication exchanger for sharing a secret key for secret communication used for secret communication with the other encryptor through the Internet, with the other encryptor by using the public key included in the communication management table of the encryptor side" (page. 9).

A substitute specification in proper idiomatic English and in compliance with 37 CFR 1.52(a) and (b) is required. The substitute specification filed must be accompanied by a statement that it contains no new matter.

Claim Objections

Claim 3 is objected to because of the following informalities: Line 14, should read "to be *stored* in the encryptor" instead of "to be *store* in the encryptor". Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1 and 12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 and 12 recite the limitation "the encryptor" in lines 25 and 36 (claim 1) and lines 16, 25, 28 (claim 12). There is insufficient antecedent basis for this limitation in the claim. For the purposes of examination, it will be presumed that the applicant is referring to "an encryptor".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 – 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arrow et al., "Method and Apparatus for Configuring a Virtual Private Network", U.S. Patent 6,226,751 B1 in view of Matchefts et al., "System for Updating Selected Part of Configuration Information Stored in a Memory of a Network Element Depending on Status of Received State Variable", U.S. Patent 6,128,656.

Arrow et al. discloses a system for allowing the flexible creation and modification of virtual private networks (Arrow et al., col. 3, lines 39-41). The system comprises a plurality of virtual private network units ('encryptors'), which are managed by a VPN management station ('manager') (Arrow et al., Abstract; Fig. 1). The VPN units are used to encrypt and secure communications over a public network (Arrow et al., col. 2, lines 29-30, 50-67; col. 3, lines 8-16). The VPN management station controls the VPN units by managing the communication management information necessary for communication between units (Arrow et al., col. 6, lines 1-3). VPN units store communication management information in tables residing in memory (Arrow et al., col. 7, lines 1,2; col. 8, lines 28-38). Thus, Arrow et al. describes a VPN system comprising plural encryptors and a manager for creating virtual private networks over a public network and for communicating communication management information between encryptors and the manager. However, Arrow et al., does not detail the system components necessary to maintain concurrency of the communication management

information contained by the plural encryptors and the manager (Arrow et al., col. 7, lines 65, 66).

Matchefts et al. discloses system components for maintaining concurrency of communication management information in a system comprising network devices and a network manager. To affect consistency of communication management information, the network manager installs and updates the communication management information in the network devices as well as maintains a storage means for keeping the reconciled communication management information of each device (Matchefts et al., col. 1, lines 47-59; col.3, lines 1-4). Most notably, Matchefts discloses the use of network device tables containing network communication management information, including variables used to identify the timeliness of the information (Matchefts et al., col. 3, lines 34-51). Also, Matchefts et al. discloses a network manager that examines the communication management tables of a network device, and decides to perform synchronization operations depending on the identifiers ("variables") contained within the tables (Matchefts et al., col. 5, line 65 – col. 6, line 8). Thus, Matchefts et al. describes system components usable in a network system for maintaining concurrency of network communication management information.

It would be obvious to one of ordinary skill in the art to combine the configuration concurrency components of Matchefts et al. with the VPN system of Arrow et al. because it is obvious that a system for dynamically establishing and configuring network elements would also need components for establishing conformity of network

information so that communications over the public network between a plurality of elements can be maintained.

Regarding claim 1, the combination of Arrow et al. and Matchefts et al. disclose a communication management table transfer system comprising:

plural encryptors connected to each other through Internet (Arrow et al., Fig. 1, elems. 115, 125, 100).

a manager which manages the communication management table used for communication among the plural encryptors (Matchefts et al., col. 5, line 65 – col. 6, line 8).

wherein each of the plural encryptors includes:

a communication management table memory of an encryptor side for storing a communication management table of the encryptor side which is the communication management table to be stored in the each of the plural encryptors (Matchefts et al., col. 3, lines 15-19).

communication management table version memory of the encryptor side for storing a communication management table version of the encryptor side which is a version of the communication management table of the encryptor side (Matchefts et al., col. 3, lines 34-51; col. 6, lines 4-8, 57-62). As shown by Matchefts et al., the table stored in memory, contains variables used to identify the timeliness of the contained information. Based upon these variables, the

manager can choose to update the communication management information. Thus, these variables serve the purpose as version identifiers.

and a communication management table version sender for sending the communication management table version of the encryptor side to the manager The combination of Arrow et al. and Matchefts et al. shows the sending/receiving means for the encryptors (Arrow et al., Fig. 7, elems. 717, 719). It also discloses that the encryptors send to the manager communication management information including version identifying variables (Matchefts et al., Abstract).

wherein the manager includes:

a communication management table memory of a manger side for storing a communication management table of the manager side which is the communication management table to be stored in the manager (Matchefts et al., Fig. 1, elems. 14, 30, 32).

a communication management table version memory of the manager side for storing a communication management table version of the manager side which is a version of the communication management table of the manager side (Matchefts et al., Abstract). As disclosed, the manager contains along with the communication management information tables in memory, stored version identifying variables.

a communication management table version receiver for receiving the communication management table version of the encryptor side from the encryptor (Matchefts et al., Fig. 2, elems. 50, 56).

a communication management table version checker for checking and finding mismatch of the communication management table version of the encryptor side received and the communication management table version of the manager side (Matchefts et al., Fig. 2, elems. 56; col. 6, lines 4-7).

a communication management table sender for sending the communication management table of the manager side when the mismatch is found by the communication management table version checker (Matchefts et al., col. 6, lines 30-36).

wherein an encryptor further includes a communication management table receiver for receiving the communication management table of the manager side from the manager. The combination of Arrow et al. and Matchefts et al. shows the sending/receiving means for the encryptors (Arrow et al., Fig. 7, elems. 717, 719). It also discloses that the encryptors receive from the manager network configuration information to be stored in tables (Matchefts et al., col. 3, lines 1-20).

and wherein the communication management table memory of the encryptor side stores the communication management table of the manager side received by the communication management table receiver as the communication management table of the encryptor side (Matchefts et al., col. 3, lines 1-20, 34-51).

Regarding claim 2, the combination of Arrow et al. and Matchefts et al. disclose:

wherein the communication management table sender further sends the

communication management table version of the manager side when the mismatch is found by the communication management table version checker (Matchefts et al., Fig. 2, elems. 56; col. 6, lines 4-7, 30-36).

wherein the communication management table receiver further receives the communication management table version of the manager side from the manager (Matchefts et al., col. 3, lines 1-20;). The combination of Arrow et al. and Matchefts et al. discloses that the encryptors receive from the manager network configuration information to be stored in tables. Because the tables contain version identifying variables, a concurrency update with the manager would cause the encryptors to receive updated version identifying variables.

wherein the communication management table version memory of the encryptor side stores the communication management table version of the manager side received by the communication management table receiver as the communication management table version of the encryptor side (Matchefts et al., col. 3, lines 1-20;).

Regarding claim 3, the combination of Arrow et al. and Matchefts et al. disclose a manager managing a communication management table used for communication among plural encryptors connected to each other through Internet comprising:

a communication management table memory of a manger side for storing a communication management table of the manager side which is the communication management table to be stored in the manager (Matchefts et al., Fig. 1, elems. 14, 30, 32).

a communication management table version memory of the manager side for storing a communication management table version of the manager side which is a version of the communication management table of the manager (Matchefts et al., Abstract). As disclosed, the manager contains along with the communication management information tables in memory, stored version identifying variables.

a communication management table version receiver for receiving a communication management table version of an encryptor side which is a version of the communication management table of the encryptor side to be store in the encryptor from each of the plural encryptors (Matchefts et al., Fig. 2, elems. 50, 56).

a communication management table version checker for checking and finding mismatch of the communication management table version of the encryptor side received and the communication management table version of the manager side (Matchefts et al., Fig. 2, elems. 56; col. 6, lines 4-7).

and communication management table sender for sending the communication management table of the manager side when the mismatch is found by the communication management table version checker (Matchefts et al., col. 6, lines 30-36).

Regarding claim 4, the combination of Arrow et al. and Matchefts et al. disclose

wherein the communication management table sender further sends the communication management table version of the manager side when the mismatch is found by the communication management table version checker (Matchefts et al., col. 6, lines 30-36).

Regarding claim 5, the combination of Arrow et al. and Matchefts et al. disclose *a communication management table updater of the manager side for updating the communication management table of the manager side and the communication management table version the manager side correspondingly* (Matchefts et al., Fig. 2, elem. 56; col. 6, lines 4-7). The network monitor performs the functions of a table updater.

Regarding claim 6, the combination of Arrow et al. and Matchefts et al. disclose *a communication management table update information receiver for receiving communication management table update information which is information to be updated within the communication management table of the manager side* (Matchefts et al., Fig. 2, elem. 56; col. 6, lines 4-7). The network monitor performs the functions of a table update receiver.

Regarding claim 7, it recites the limitations pertaining to the encryptor portion of claim 1, and is therefore rejected for the same reasons.

Regarding claim 8, it recites the limitations of claim 2, and is therefore rejected for the same reasons.

Regarding claims 9 and 10, the combination of Arrow et al. and Matchefts et al. disclose *wherein the communication management table includes a public key* (Arrow et al., col. 10, lines 7-17). The encryptors use public key cryptography in the process of securing of communications (Arrow et al., col. 10, lines 7-10). Further, encryptors store in communication management tables the unique identification and communication information (i.e. addresses, encryption algorithms, and key management information) of other encryptors. Thus, it is obvious that the tables would include the unique public keys usable for communication between encryptors.

Also disclosed is a secret key and certificate exchanger (Arrow et al., col. 10, lines 7-20). The RSA module ("*secret/certification key for secret key communication exchanger*") along with the Key management module supports the encryption and certification of communications by setting up and exchanging certificates and keys.

Regarding claim 10, it is rejected for the same reason as claim 9.

Regarding claim 11, the combination of Arrow et al. and Matchefts et al. disclose wherein:

the other encryptor is connected to a subnet (Arrow et al., Fig. 1, elem. 110).

the communication management table includes subnet configuration information which is information related to a configuration of the subnet (Arrow et al., col. 7, lines 26-40).

the encryptor further comprising:

an Internet communicating unit for communicating with the other encryptor through the Internet based on the subnet configuration information included in the communication management table of the encryptor side (Arrow et al., col. 10, lines 31-42).

Regarding claim 12, the combination of Arrow et al. and Matchefts et al. disclose a method for transferring a communication management table used for a communication management table transfer system including:

plural encryptors connected to each other through Internet (Arrow et al., Fig. 1, elems. 115, 125, 100).

each of which has a communication management table memory of an encryptor side for storing a communication management table of the encryptor side and a communication management table version memory for storing a communication management table version of the encryptor side (Matchefts et al., col. 3, lines 15-19).

a manager managing the communication management table used for communication among the plural encryptors, which has a communication management table memory of a manager side for storing a communication management table of the manager side and a communication management table version memory for storing a

communication management table version of the manager side (Matchefts et al., Fig. 1, elems. 14, 30, 32).

the method comprising:

sending the communication management table version of the encryptor side to the manager by the encryptor (Matchefts et al., Abstract).

receiving the communication management table version of encryptor side from the encryptor by the manager (Matchefts et al., col. 5, line 64 – col. 6, line 8).

checking and finding mismatch of the communication management table version of the encryptor side received and the communication management table version of the manager side by the manager (Matchefts et al., col. 5, line 64 – col. 6, line 8).

sending the communication management table of the manager side by the manager when the mismatch is found by the checking and finding (Matchefts et al., col. 6, lines 30-36).

receiving the communication management table of the manager side from the manager by the encryptor. The combination of Arrow et al. and Matchefts et al. shows the sending/receiving means for the encryptors (Arrow et al., Fig. 7, elems. 717, 719). It also discloses that the encryptors receive from the manager network configuration information to be stored in tables (Matchefts et al., col. 3, lines 1-20).

and storing the communication management table of the manager side received as the communication management table of the encryptor side by the encryptor (Matchefts et al., col. 3, lines 1-20, 34-51).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached at (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER